AF
IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	: Anat Bremler BAR, et al.	Examiner : Thuong Nguyen
Serial No.:	10/774,169	Group Art Unit: 2455
Filed:	February 5, 2004	Confirm No.: 7298

For: DETECTING AND PROTECTING AGAINST WORM TRAFFIC ON A NETWORK

REPLY BRIEF PURSUANT TO 37 C.F.R. § 41.41

Mail Stop - Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 41.41, the Appellant respectfully submits this Reply Brief in response to the Examiner's Answer mailed January 15, 2009. Entry of this Reply Brief is respectfully requested.

REFERENCED DOCUMENTS

The following documents are referenced herein:

Office Action mailed April 29, 2008 ("Office Action")

Applicant's Appeal Brief filed November 11, 2008 ("Brief")

Examiner's Answer to the Brief, mailed January 15, 2009 ("Answer")

US Patent No. 6,886,102 to Lyle, cited as prior art by the Examiner ("Lyle")

US Patent No. 6,886,099 to Smithson, cited as prior art by the Examiner ("Smithson)

STATUS OF CLAIMS

Claims 1, 4 – 24, 29 – 35, 38 – 58, 63 – 69, 72 – 92, and 97 – 108 are pending. The application was filed with 102 claims. Claims 103 – 108 were added in the response filed on July 19, 2006. Claims 2 – 3, 27, 36 – 37, 61, 70 – 71, and 95 were canceled in the response filed July 19, 2006. Claims 25 – 26, 28, 59 – 60, 62, 93 – 94, and 96 were canceled in the response after final filed October 10, 2007.

The rejection of claims 1, 4 – 24, 29 – 35, 38 – 58, 63 – 69, 72 – 92, and 97 – 108 is being appealed.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed are as follows:

1. Rejection of independent claim 1 under 35 U.S.C. § 103(a) over Lyle in view of Smithson;
2. Rejection of independent claim 29 under 35 U.S.C. § 103(a) over Lyle in view of Smithson;
3. Rejection of independent claim 32 under 35 U.S.C. § 103(a) over Lyle in view of Smithson;
4. Rejection of independent claim 35 under 35 U.S.C. § 103(a) over Lyle in view of Smithson;
5. Rejection of independent claim 63 under 35 U.S.C. § 103(a) over Lyle in view of Smithson;
6. Rejection of independent claim 66 under 35 U.S.C. § 103(a) over Lyle in view of Smithson;
7. Rejection of independent claim 69 under 35 U.S.C. § 103(a) over Lyle in view of Smithson;
8. Rejection of independent claim 97 under 35 U.S.C. § 103(a) over Lyle in view of Smithson;
9. Rejection of independent claim 100 under 35 U.S.C. § 103(a) over Lyle in view of Smithson.

The Appellant believes that the Examiner's application of the prior art is not appropriate and that the present claims are novel and non-obvious over the cited prior art.

ARGUMENT

In the "Response to Argument" of the Examiner's Answer (page 47), the Examiner responds to the Appellant's arguments as set forth in the Appeal Brief dated November 6, 2008. In reply, the Appellant maintains that the present invention, as claimed, is patentable over the applied references at least based on the previously-submitted arguments and the arguments set forth below.

1. Neither Lyle nor Smithson, either alone or in combination, renders independent claims 1, 35, and 69 unpatentable.

   The following limitation is recited in independent claims 1, 35, and 69:

   > "identifying a subset of the group of the address such that the addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the group;"

   a. Claims 1, 35, and 69 are rejected by the Examiner under 35 USC 103 (a) as being unpatentable over Lyle in view of Smithson [e.g., OA point 4, pg. 3 - 4]. The Examiner acknowledges that Lyle fails to teach identifying a subset expected to receive smaller amounts of communication traffic, but states that this limitation is taught by Smithson [Smithson Fig. 2; col. 4 lines 5-25; col. 5 lines 7 - 23].

   b. The rejection is traversed [Brief pg. 10] on the grounds that Smithson fails to teach or reasonably suggest identifying a subset of addresses expected to receive smaller amounts of communication traffic. The cited excerpts of Smithson [Fig. 2; col. 4 lines 5-25; col. 5 lines 7 - 23] disclose the use of thresholds to detect exceeding a threshold, not determining a subset of addresses on a network that receive a smaller amount of communication traffic than others.

   c. In the Answer, the Examiner supports the rejection by arguing that Smithson's method "periodically checks each of the measurement parameters against its respective threshold..." and that Smithson discloses a

method of testing the threshold to determine if the signal indicates a virus outbreak. [Answer pg. 47-48].

d. The Appellant disagrees as follows:

Smithson fails to explicitly teach identifying a subset of addresses expected to receive smaller amounts of communication traffic. The Examiner states that Smithson discloses periodically checking measurement parameters against a threshold, but provides no details showing how this suggests the above limitation of identifying a subset of addresses.

The Examiner's argument regarding Smithson's thresholds appears to be that periodically checking each of the measurement parameters for the various addresses against their respective threshold yields the same result as identifying a subset of the addresses receiving smaller amounts of the communication traffic. That is, the Examiner's argument appears to be that addresses which do not exceed a given traffic volume threshold are expected to receive smaller amounts of traffic than addresses which do exceed the threshold.

However, there is *no functional or structural equivalence* between not exceeding such a threshold and being a member of a subset expected to receive smaller amounts of traffic. Consider, for example, a case where *none* of the addresses exceed the threshold. In this case, the entire set of addresses is below the threshold, and Smithson fails to provide any identification of a subset of addresses. This is also true in the case where *all* of the addresses exceed the threshold. Thus, discriminating addresses according to a threshold does not meet the limitation of identifying a subset of addresses expected to receive smaller amounts of communication traffic, as recited in claims 1, 35, and 69.

Smithson not only fails to disclose or reasonably suggest using the thresholds to identify subsets of addresses, but also uses thresholds in an

entirely different manner, for identifying virus outbreaks. The Examiner's argument proposing that Smithson's threshold discrimination can be used for identifying a subset of addresses which are expected to receive smaller amounts of communication traffic is tantamount to making a modification that changes the principle of operation of the Smithson reference, which is not allowed under MPEP 2143.01.

The above points show that Lyle in view of Smithson does not meet independent claims 1, 35, and 69. The Appellant continues to maintain that independent claims 1, 35, and 69, and claims depending therefrom are patentable over the cited prior art.

2. Neither Lyle nor Smithson, either alone or in combination, renders independent claims 29, 63, and 97 unpatentable.

The following limitations are recited in independent claims 29, 63, and 97:

> "monitoring the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection;"
>
> "detecting an increase in a rate of arrival of the packets that are indicative of a communication failure;"
>
> "responsively to the increase, filtering the communication traffic so as to remove at least a portion ... that is generated by the worm infection."

a. Claims 29, 63, and 97 are rejected by the Examiner under 35 USC 103 (a) as being unpatentable over Lyle in view of Smithson [e.g., OA point 18, pg. 8 - 9], based on the following arguments:

> The Examiner states that Lyle discloses a method of monitoring the network traffic for suspicious data in the sense that it indicates that an attack may be taking place [Lyle col. 10 lines 53-59].
>
> The Examiner further states that Lyle discloses determining if the rate of certain types of messages exceeds a normal level [Lyle col. 10 line 60 - col. 11 line 1].
>
> The Examiner acknowledges that Lyle fails to teach the claim limitation, "responsively to the increase, filtering the communication traffic so as to remove at least a portion ... that is generated by the worm infection". But the Examiner states that Smithson teaches this limitation [Smithson Figure 23; col. 6 lines 34 - 43].

b. The rejection is traversed [Brief pg. 11] on the following grounds:

Lyle relates only to detecting the level or rate of certain types of messages without specifying the types of messages that are involved. Thus, Lyle fails to disclose detecting packets that are indicative of a communication failure in the network that is characteristic of a worm infection.

Lyle fails to teach or suggest how the level or rate of communication traffic is related to communication failures. Thus, Lyle fails to disclose or suggest detecting a communication failure.

Lyle fails to teach or suggest that data packets indicative of communication failures can be detected.

Smithson fails to teach or suggest detecting packets of any particular type, including packets indicative of a communication failure.

c. In the Answer, the Examiner supports the rejection by arguing that Lyle discloses a method of scanning, detecting, and determining suspicious data or whether an attack may be taking place by detecting the number {of times} the rate is exceeded during a predetermined period of time [Answer page 48, second paragraph].

d. The Appellant disagrees for the following reasons:

Detecting of packets which are indicative of a communication failure is neither taught nor reasonably suggested in either Lyle or Smithson, or the combination thereof.

Detecting whether or how frequently a rate exceeds a normal level (Lyle) is *not* equivalent to detecting an increase in the rate (present claims 29, 63, and 97). First, the rate can increase without exceeding the normal level. Second, if the rate happens to exceed the normal level, the rate can continue to exceed the normal level without increasing; in fact, the rate can actually decrease while continuing to exceed the normal level.

The above points show that Lyle in view of Smithson does not meet independent claims 29, 63, and 97. The Appellant continues to maintain that independent claims 29, 63, and 97, and claims depending therefrom are patentable over the cited prior art.

3. Neither Lyle nor Smithson, either alone or in combination, renders independent claims 32, 66, and 100 unpatentable.

The following limitations are recited in independent claims 32, 66, and 100:

> "monitoring the communication traffic on a network so as to detect ill-formed packets;"
>
> "making a determination, responsively to the ill-formed packets, that at least a portion of the communication traffic has been generated by the worm infection;"
>
> "responsively to the determination, filtering the communication traffic so as to remove at least the portion of the communication traffic that is generated by the worm infection;"

a. Claims 32, 66, and 100 are rejected by the Examiner under 35 USC 103 (a) as being unpatentable over Lyle in view of Smithson [e.g., OA point 21, pg. 9 - 10], based on the following arguments:

> The Examiner states that Lyle discloses a method of scanning the network for suspicious data [Lyle col. 7 lines 9 - 19].
>
> The Examiner further states that Lyle discloses a method where an alerting module issues an alert in case an attack is detected [Lyle col. 8 lines 26 - 39].
>
> The Examiner acknowledges that Lyle fails to teach the claim limitation, "responsively to the determination, filtering the communication traffic so as to remove at least the portion ... generated by the worm infection". But the Examiner states that Smithson teaches this limitation [Smithson Figure 23, col. 6 lines 34 - 43].

b. The rejection is traversed [Brief pg. 12] on the grounds that Both Lyle and Smithson fail to disclose or reasonably suggest that data packets can be ill-

formed or detecting ill-formed packets to determine that a worm infection has occurred.

c. In the Answer, the Examiner acknowledges that Lyle does not disclose "ill-formed packets", but supports the rejection by arguing that it is obvious to assume that suspicious packets or a potential attack could be an ill-formed packet [Answer pg. 49]

d. The Appellant disagrees as follows:

Scanning for suspicious data (Lyle) does not necessarily include scanning for worms (present claims 32, 66, and 100). There are classes of suspicious data objects besides worms (e.g., viruses, spam, phishing attacks, etc.).

Smithson [Smithson Figure 23, col. 6 lines 34 - 43] discloses blocking e-mail messages which are infected with viruses or have attachments containing viruses. In doing so, Smithson blocks data objects which are individually-identifiable because they contain malicious code (a virus). However, filtering traffic generated by a worm infection (present claims 32, 66, and 100) is *not* the same as blocking a virus, because the traffic data objects generated by the worm infection do not necessarily contain malicious code and are therefore not necessarily individually-identifiable as required for Smithson to detect. As disclosed in the present application [paragraph 0004], traffic generated by a worm infection may involve innocuous messages (e.g., TCP SYN request packets) which individually have no malicious content. Smithson is therefore unable to detect and block worm infection traffic. Thus, Lyle in view of Smithson fails to meet present claims 32, 66, and 100.

Moreover, Appellant submits that at the time the present invention was made, it would *not* have been obvious to a person of ordinary skill in the art that ill-formed data packets are related to worm infections. The

Examiner does not substantiate the contention of obviousness with any prior art references.

The above points show that Lyle in view of Smithson does not meet independent claims 32, 66, and 100. The Appellant continues to maintain that independent claims 32, 66, and 100, and claims depending therefrom, are patentable over the cited prior art.

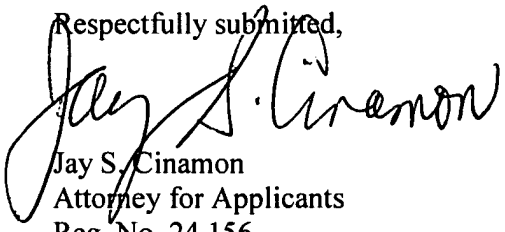
CONCLUSION

The above arguments show that neither Lyle nor Smithson, either alone or in combination, renders independent claims 1, 29, 32, 35, 63, 66, 69, 97, and 100 unpatentable. All other claims of the present application depend from the aforementioned independent claims, and therefore Lyle and Smithson, alone or in combination, fail to render the present claims unpatentable.

For the above reasons, as well as the reasons set forth in the Appeal Brief, the Appellant respectfully requests that the Board reverse the Examiner's rejections of all claims on Appeal. An early and favorable decision on the merits of the Appeal is respectfully requested.

Please charge any fees which may be due and which have not been submitted herewith to our Deposit Account No. 01-0035.

Respectfully submitted,



Jay S. Cinamon
Attorney for Applicants
Reg. No. 24,156

ABELMAN, FRAYNE & SCHWAB
666 THIRD AVENUE, 10TH FLOOR
NEW YORK, NEW YORK 10017
Tel: (212) 949-9022
Direct: (212 885-9232
Fax: (212) 949-9190